Statement

of

David Z. Bodenheimer, Esq.

Partner
Crowell & Moring LLP
Washington, DC

Before the

House Armed Services Committee's
Subcommittee on Terrorism,
Unconventional Threats and Capabilities

Concerning

Private Sector Perspectives on
Department of Defense
Information Technology and Cybersecurity Activities

February 10, 2010

Introduction

Ms. Chairwoman Sanchez and Members of the Committee. Thank you for holding these hearings today to seek Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities. The Department of Defense has long been on the leading edge in advancing technology, harnessing information, and developing acquisition policy. Never has there been a more critical time for the Department of Defense to demonstrate its leadership than now on cybersecurity. The stakes are simply too great to wait.

And industry must be an essential partner in hardening our defenses against cyber attack. As Director of National Intelligence Dennis Blair aptly stated in the 2010 Annual Threat Assessment, "acting independently, neither the US Government nor the private sector can fully control or protect the country's information infrastructure."[1] Quite bluntly, the Defense Department and industry will either succeed together – or fail separately.

For this vital partnership between the Defense Department and industry, what are the critical ingredients? Among other needs, the essentials include:

- Effective Information Sharing. To connect the dots effectively, cybersecurity information sharing must be a two-way street, with much broader industry participation and more carrots – and fewer sticks – for industry information sharing.

- Cyber Standards – Clear, Firm, and Consistent. The Defense Department should seize the opportunity to define clear, firm, and consistent cybersecurity standards that become the gold standard on which other agencies and industries can converge.

- Breakthrough Technologies. For effective cybersecurity that we can trust and afford, breakthrough technologies remain indispensable, requiring a combination of more R&D funding, public-private innovation rewards, and technology clearinghouses to bring the best and brightest to building our cyber defenses.

- Liability Limitations. Just as Congress fostered technology advances through the SAFETY Act's liability limitations for anti-terrorism technology, such protections should be shaped to encourage greater technology development and broader information sharing for the cybersecurity industry.

---

[1] Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence*, p. 2 (Feb. 3, 2010) (http://www.dni.gov/testimonies/20100202_testimony.pdf).

I am David Bodenheimer, a partner in the law firm of Crowell & Moring LLP in Washington, DC where I lead the Homeland Security practice and specialize in government contracts. As part of this practice, I have advised clients, published articles, and lectured extensively on cybersecurity and government contract matters. In addition, I serve as Co Vice-Chair of the ABA Cybersecurity Committee and Co-Chair of the ABA Homeland Security Committee. Prior to entering private practice, I served six years (1982-88) as a civilian attorney for the Department of the Navy where I handled a broad spectrum of government contract matters in the field, at the Commands, and as Assistant to the General Counsel. However, I appear before your Committee today in my personal capacity and the views that I express are my own.

I. Why We Must Act Now to Protect Our Information Assets

Simply waiting for the cyber apocalypse or digital Pearl Harbor is not an option. Virtual unanimity exists that we need to take action now – if not last year.

- Senators Rockefeller and Snowe. "We need to act now – the time to combat cyber terror was yesterday."[2]
- President Obama. "The status quo is no longer acceptable."[3]
- Industry. "Quite frankly, the bad guys are winning."[4]
- CSIS Cyber Report. "America's failure to protect cyberspace is one of the most urgent national security problems . . . ."[5]

No real dispute remains about the gravity of the threat or the urgency for taking action to guard our information assets. By any measure, the record of cyber attacks, security breaches, and compromised data is alarming. These threats strike at our national security, economic well-being, and personal privacy.

---

[2] "Chairman Rockefeller and Senator Snowe's Statement on the Obama Administration's Cybersecurity Review," Senate Committee on Commerce, Science, and Transportation (May 29, 2009).

[3] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

[4] *Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information? Hearings Before Senate Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the Comm. on Homeland Security & Governmental Affairs*, 110th Cong., p. 28 (Mar. 12, 2008) (statement of Mr. Tim Bennett, Cyber Security Industry Alliance).

[5] CSIS Commission on Cybersecurity, *Securing Cyberspace for the 44th Presidency*, p. 11 (Dec. 2008) (hereinafter CSIS Commission Report).

National Security Threats. As its "one central finding," the CSIS Commission on Cybersecurity warned that the "United States must treat cybersecurity as one of the most important national security challenges it faces."[6] In January 2009, former DNI Director Mike McConnell "equated 'cyber weapons' with weapons of mass destruction when he expressed concern about terrorists' use of technology to degrade the nation's infrastructure."[7] Recent history has already underscored the gravity and reach of this threat.

- 2007 Foreign Intrusions. "The damage from cyber attack is real. In 2007, the Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities."[8]

- 2008 Malware Attack. "In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected last year by malicious software – malware."[9]

- Presidential Helicopter. "The U.S. Navy is investigating how an unauthorized user in Iran gained online access to blueprints and other information about a helicopter in President Obama's fleet."[10]

- 360 Million Attacks. "Last year the Pentagon reported more than 360 million attempts to break into its networks."[11]

- Russian Cyber Attacks. "And last year we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, cyber attacks crippled Georgian government websites."[12]

---

[6] CSIS Commission Report, p. 15 (Dec. 2008).

[7] Congressional Research Service (CRS), "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," CRS Report R40427, p. 3 (Mar. 10, 2009) (hereinafter CRS CNCI Report).

[8] CSIS Commission on Report, p. 12 (Dec. 2008).

[9] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

[10] "Source in Iran Sees Plans for President's Chopper," *USA Today* (Mar. 2, 2009).

[11] "Subcommittee Chairman Lipinski's Floor Speech on H.R. 4061," House Subcomm. on Science and Technology (Feb. 3, 2010) (http://science.house.gov/press/PRArticle.aspx?NewsID=2736).

[12] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

Economic Damage. Cyber attacks also steal our critical technology and trade secrets, sapping the economic power that fuels our military might. As stated in the President's Cyberspace Policy Review, "[o]ur digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information."[13] For such security breaches, the economic stakes are enormous:

> According to a 2009 report from McAfee, the 2008 overall losses from data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage last year. Respondents estimated that they lost data worth a total of $4.6 billion and spent about $600 million cleaning up after breaches.[14]

Even these losses pale in comparison to the catastrophic economic damage that could result from an attack on America's critical infrastructure, such as the power grid or financial system.[15]

Personal Impact. Security breaches also strike with the unpleasant personal force of a punch in the gut, violating privacy and stealing identities. Since 2005, the Privacy Rights Clearinghouse has reported 345,124,400 records with sensitive personal information being compromised in security breaches – with over 80 million records compromised within the last 6 months.[16] Service men and women, veterans, and their families have been hit particularly hard.

- 26 Million Veterans. "In May 2006, the Department of Veterans Affairs lost an unsecured laptop computer hard drive containing the health records and other sensitive personal information of approximately 26.5 million veterans and their spouses."[17]

---

[13] President's Report, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, p. i (May 2009).

[14] *Do the Payment Card Industry Data Standards Reduce Cybercrime? Hearings Before the House Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology of Comm. on Homeland Security*, 111th Cong. (Mar. 31, 2009) (statement of Chairman Thompson) (http://homeland.house.gov/SiteDocuments/20090331141926-86082.pdf).

[15] CRS CNCI Report, p. 3 (potential for "strategic damage to the United States"); Wright, "The Spymaster: Can Mike McConnell fix America's Intelligence Community," *The New Yorker*, p. 51 (Jan. 21, 2008) (". . . McConnell then said, 'If the 9/11 perpetrators had focused on a single U.S. bank through cyber-attack and it had been successful, it would have an order-of-magnitude greater impact on the U.S. economy'").

[16] Privacy Rights Clearinghouse, "Chronology of Data Breaches" (Feb. 4, 2010) compared with 262,442,156 records compromised through June 11, 2009 (http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP).

[17] S. REP No. 111-110, p. 3 (Dec. 17, 2009).

- 2008 Walter Reed Breach. "In June 2008, the Walter Reed Army Medical Center reported that officials were investigating the possible disclosure of personally identifiable information through unauthorized sharing of a data file containing the names of approximately 1,000 Military Health System beneficiaries."[18]

- Navy CIO Victimized. "The personal identifiable information of the Navy chief information officer has been compromised, again. And, it isn't just the second or third or fourth or even fifth time Robert Carey's PII has been exposed, but the sixth instance."[19]

- Defense Secretary Hacked. "The Secretary of Defense's unclassified e-mail was hacked."[20]

In summary, cyber assaults threaten our military might, economic power, and personal well-being. And it will get much worse – perhaps cataclysmically so – if treated as a middle-of-the-inbox inconvenience rather than as the clear and present danger now hanging over our collective heads.

II. Why Public-Private Partnerships Are Critical to Cyber Defense

Hardly anyone disputes the paramount importance of public-private partnerships, particularly given that the bulk of our critical information assets reside in the hands of the private sector. More than many agencies, the Defense Department has made great strides in recognizing the need for private-sector involvement though the use of bilateral understandings struck with some military contractors. The time is ripe for the Defense Department to expand these private-sector relationships into a full public-private partnership.

A. The Need for Full Public-Private Partnerships

For at least three reasons, the Defense Department and its contractors must band together to succeed in defending our cyber assets and security: (1) nearly everyone agrees that public-private partnerships are essential to effective cyber defense; (2) the private sector holds the

---

[18] Government Accountability Office (GAO), "Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses," p. 9 (GAO-09-546) (July 2009).

[19] Chabrow, "Navy CIO's PII Exposed for Sixth Time," *Government Information Security News* (Jan. 4, 2010) (http://blogs.govinfosecurity.com/posts.php?postID=404&rf=010510eg).

[20] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 8 (Mar. 19, 2009) (statement of Dr. James Lewis).

overwhelming majority of critical information infrastructure; and (3) public-private partnerships have been the model for success during past national crises.

1. The Consensus on the Need for Public-Private Partnership

Virtually every top official, cybersecurity expert, and major review has reached the same conclusion – public-private partnerships are vital to any successful cybersecurity strategy. Even a short sample reflects this consensus.

- President Obama. "Third, we will strengthen the public/private partnerships that are critical to this [cybersecurity] endeavor."[21]

- Senator Rockefeller. "We need a coordinated public-private response. Currently, this does not exist."[22]

- Representative Lipinski. "Improving the security of cyberspace is of the utmost importance and it will take the collective effort of the Federal government, private sector, our scientists and engineers, and every American to succeed."[23]

- DNI Director Blair. "Acting independently, neither the U.S. government nor the private sector can fully control or protect the country's information infrastructure."[24]

- CSIS Report. "The U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and responsive activities."[25]

---

[21] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

[22] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation*, 111th Cong., p. 2 (Mar. 19, 2009) (statement of Sen. Rockefeller).

[23] "Subcommittee Chairman Lipinski's Floor Speech on H.R. 4061," House Subcomm. on Science and Technology (Feb. 3, 2010) (http://science.house.gov/press/PRArticle.aspx?NewsID=2736).

[24] Blair, "Director of National Intelligence's Annual Threat Assessment," *Government Info Security* (Feb. 2, 2010) (http://www.govinfosecurity.com/articles.php?art_id=2154&rf=011610eg).

[25] CSIS Commission Report, p. 6 (Dec. 2008).

- Industry. "[G]overnment and industry must develop a much more thoughtful, fundamental and contemporary relationship to address their mutual (not just government's) cyber security needs."[26]

- Experts Generally. "The key strategy improvements identified by cybersecurity experts [include]: . . . Bolster public-private partnerships through an improved value proposition and use of incentives."[27]

While this list could be much longer, the conclusion would remain the same – the public and private sectors must be partners in the quest for an effective and affordable cybersecurity strategy. Without a partnership, even the most elegant solution will fall short, leaving both the public and private sector exposed to ever more devastating cyber attacks.

2. The Private Sector's Information Infrastructure

Even without such a consensus, the need for public-private partnership would still be inevitable. Neither the public nor private sector control the entire information infrastructure, yet the public and private networks are both intertwined and interdependent. In its report, the CSIS Commission summed up the rationale for why the public and private sectors must be partners in securing cyberspace:

> Securing cyberspace requires government and the private sector to work together. The private sector designs, deploys, and maintains much of the nation's critical infrastructure. This is important because unlike certain other elements of national security, cyberspace cannot be secured by the government alone. There is a bifurcation of responsibility (the government must protect national security) and control (it does not manage the asset or provide the function that must be protected).[28]

3. The Historical Success of Public-Private Partnerships

During the bleakest of times, the United States military and its contractors have teamed up to defeat foes that literally threatened the survival of the free world. In 1946, Army Chief of Staff Eisenhower described the effectiveness of this partnership during World War II:

---

[26] Internet Security Alliance, "The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress," p. 3 (2008).

[27] GAO, "Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats," p. 15 (GAO-10-230T) (Nov. 17, 2009).

[28] CSIS Commission Report, p. 43 (Dec. 2008).

> The armed forces could not have won the war alone. Scientists and business men contributed techniques and weapons which enabled us to outwit and overwhelm the enemy. Their understanding of the Army's needs made possible the highest degree of cooperation. This pattern of integration must be translated into a peacetime counterpart which will not merely familiarize the Army with the progress made in science and industry, but draw into our planning for national security all the civilian resources which can contribute to the defense of the country.[29]

Some may say that the threat is not the same as during World War II. In some ways, today's threat is even greater because the cyber barbarians can now strike at the heart of America in ways that the Nazis and Japanese could not in the 1940s.

> [Cybersecurity is] about protecting our Nation's critical infrastructure from cyberattacks that could severely impact commerce and the economy in absolutely devastating ways.
>
> * * *
>
> For example, private-sector IT systems control virtually all of this critical infrastructure; traffic lights, rail networks. It would be very easy to make train switches so that two trains collide, affect or disrupt water and electricity, or release water from dams, where the computers are involved. How our money moves, they could stop that. Any part of the country, all of the country is vulnerable.[30]

The magnitude of this cyber threat explains why two Directors of National Intelligence "Mike McConnell, under President Bush, and Admiral Blair, under President Obama, both said that the number-one security threat to the United States of America was cybersecurity, or cyberterror . . . ."[31] In short, just as the public-private partnership worked during World War II, the time is right to do so again to forestall a digital Pearl Harbor.

B. The Need for Expanding Defense Partnerships

Through its Defense Industrial Base (DIB) initiative, the Defense Department has established a pilot program for partnering with a portion of the defense industry. In testimony before this Subcommittee last year, Deputy Assistant Secretary Robert Lentz summarized the Defense Department's DIB program:

---

[29] Nagle, *A History of Government Contracting*, p. 464 (1992).

[30] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation*, 111th Cong., p. 2 (Mar. 19, 2009) (statement of Sen. Rockefeller).

[31] *Id.*, p. 1.

> In early 2008, the Department initiated a DIB Cyber Security and Information Assurance (CS/IA) pilot program to address cybersecurity risks to DIB unclassified networks that support DoD programs. The DIB CS/IA pilot has five major components: a binding bilateral DoD-DIB company framework agreement to facilitate CS/IA cooperation; threat and vulnerability information sharing; DIB network incident reporting; damage assessments; and DoD acquisition and contracting changes, including proposed changes to Defense Federal Acquisition Regulation Supplement (DFARS). The DoD-DIB legal framework provides the mechanism to exchange relevant threat information in a timely manner, provides intelligence and digital forensic analysis on threats, and expands Government to Industry cooperation while ensuring that industry equities and privacy are protected.[32]

While this pilot program represents a valuable start, the Defense Department now needs to move forward with a full public-private partnership. Key characteristics of this full partnership include the following:

- Broad Industry Partnership. Rather than the current bilateral model involving only a few companies, a full partnership requires broad industry participation for greater transparency and robust sharing of options, ideas, and strategy.[33]

- Timely, Two-Way Partnership. Full partnership should involve two-way exchanges before decisions have been made and strategy has already been set.[34]

---

[32] *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance: Hearings Before House Subcomm. on Terrorism, Unconventional Threats and Capabilities of Comm. on Armed Services,* 111th Cong. (May 5, 2009) (statement of Robert Lentz).

[33] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 1 (Mar. 19, 2009) ("Government engagement with industry has also often been selective, rather than open and transparent. . . . It is of great importance to industry that the government make the process of national cyber security policy-making open and transparent, so that industry participation is as broad and deep as possible, both at the classified and unclassified level").

[34] *Id.*, p. 2 (sharing "has largely been one-way"); *see also* Intelligence and National Security Alliance (INSA), "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment," p. 2 ("Create an effective public/private partnership [that will] insure that industries receive timely information that will enable them to react to attacks").

- Multi-Sector Partnership. By partnering with other sectors, DoD could leverage expertise across industries and agencies, reduce duplication caused by bilateral agreements, and benefit from existing partnerships.[35]

III. What the Private Sector Needs for Enhancing Cybersecurity Efforts

Given the escalating pace and magnitude of cyber attacks, both the public and private sectors need a new paradigm to build better cyber defenses more rapidly and cost-effectively. For this effort, five factors are key to elevating and maintaining these cyber defenses:

- Improve information sharing;
- Establish clear, firm, and consistent cybersecurity standards;
- Accelerate breakthrough cyber technologies;
- Limit liability to encourage more information sharing and technology innovation; and
- Develop mechanisms to resolve disputes fairly and quickly.

A. Effective Information Sharing

Just as the homeland security mission hinges upon information sharing ("connecting the dots"), effective cybersecurity requires real-time, two-way information sharing between the public and private sector. However, current information-sharing arrangements have consistently fallen short of what the private sector needs to fight back against cyber attacks.

- Insufficient Data. "When provided to DIB members, US Government indications and warning (I&W) intelligence frequently lacks context, is too heavily focused on domain and IP blacklisting, provides little or no finished analysis and is generally too old to constitute actionable information."[36]

- One-Way "Sharing". "To date, sharing of information about threats, vulnerabilities and attacks between industry and

---

[35] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 4, Question # 3 (Mar. 19, 2009) (Government engagement is "often based on bilateral relationships between specific agencies and specific companies or sets of companies" and "they are often redundant").

[36] Internet Security Alliance, "The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress," p. 19 (2008).

government has largely been one-way, with industry sharing information with the government."[37]

- Untimely Sharing. "Speed and timeliness of information sharing needs significant improvement for the achievement of a successful desired degree of protection and attribution."[38]

- Over-Classification. "It is also of great importance that classification be the exception rather than the norm, as it should be reserved for areas that genuinely require confidentiality."[39]

To maximize the effectiveness of information sharing with the private sector, the following three steps should be taken.

1. Engage in two-way information sharing by providing timely, actionable information, while minimizing the amount and level of classification.

2. Expand information sharing to include the broader defense industry base, rather than limiting such sharing to selected contractors with bilateral agreements.

3. Employ a carrot rather than stick approach, encouraging information sharing through incentives, rather than penalizing those who share bad news of breaches or threats.

B. Clear and Consistent Cybersecurity Standards

As a nearly universal concern, the lack of clear, firm, and consistent standards for cybersecurity has troubled the private sector. As one expert put it, "we have not brought the full power of the Federal Government to bear on the problem, and what power we did bring was applied in a fragmented and incoherent manner."[40] In another instance, the guidance has been described as "ad hoc," "redundant," and sometimes "conflicting":

---

[37] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 2, Question # 1 (Mar. 19, 2009).

[38] INSA, "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment," p. 3.

[39] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," pp. 1-2, Question # 1 (Mar. 19, 2009).

[40] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 7 (Mar. 19, 2009) (statement of Dr. James Lewis).

> We would again note that government agencies often engage the private sector in an ad hoc manner, and the engagement is often based on bilateral relationships between specific agencies and specific companies or sets of companies. As a result, they are often redundant, or in some cases conflicting, and do not effectively leverage the CIPAC [Critical Infrastructure Partnership Advisory Council] framework.[41]

A number of examples illustrate how the public and private sector can collaborate successfully to develop workable, effective standards.[42] To assure that the private sector's investment in cybersecurity compliance is directed towards cost-effective solutions, a clear, consistent, and firm set of standards is critical.

C. Breakthrough Cybersecurity Technologies

While technology is not the sole answer for achieving real cybersecurity, major advances in such technology will be critical not only for countering the ever-more sophisticated cyber threats, but also for achieving such success at a cost that the public and private sectors can bear over the long haul. To this end, President Obama stated that "we will continue to invest in cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time."[43]

For such breakthrough technologies, the investment in innovation needs to be focused in areas where market forces are less likely to drive the private sector to produce the needed technologies. Research targets include the following:

- Long-Term Research. "We need to apply more funding and support to research. And the research can't be near-term, let's-come-up-with-a-patch-for-the-latest-botnet-or-the-latest-firewall-problem, but long-term research as to how to fundamentally redesign some of the systems we're using and the security involved."[44]

---

[41] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 5, Question # 3 (Mar. 19, 2009).

[42] INSA, "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment," p. 3 (citing the Capability Maturity Model Integration (CMMI)).

[43] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

[44] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 29 (Mar. 19, 2009) (statement of Dr. Eugene Spafford).

- Basic Internet Protocols. "There needs to be Research and Development; especially in areas such as the development and implementation of new secure basic protocols for the Internet, which will not be undertaken in the private sector due to the lack of a viable business plan for implementing them profitably."[45]

- Research Coordination. "Cyber security research and development efforts in the US must be better coordinated; only through information sharing and collaboration can effective solutions emerge."[46]

- Over-Classification. "Over-classification hurts many efforts in research and public awareness."[47]

In addition to a greater focus upon cybersecurity research, other options for stimulating technology innovations include techniques embodied in the Homeland Security Act, such as agency requests for, and reviews of, "unique and innovative technologies" and the establishment of a technology "clearinghouse" for collecting and disseminating information to other agencies, as well as the private sector. *See* Pub. L. No. 107-296, § 313(b).

D. Liability Limitations and Other Incentives

The risk of lawsuits inevitably influences corporate decision-making. For cybersecurity, potential legal liability may discourage information sharing and technology development. Given the importance of both activities to the successful hardening of cyber defenses, legal safe harbors need to be considered in order to encourage greater information sharing and cyber innovation.

1. Enhancing Information Sharing

For information sharing, two factors create disincentives for making disclosures to the Government and sharing critical data with other industry partners. First, the Defense Department should explore incentives to encourage the private sector to identify security problems promptly and cooperate fully with the Defense Department to resolve such problems. In the past, some defense contractors have felt that the Defense Department's response to bad news has tended too

---

[45] Internet Security Alliance, "The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress," p. 16 (2008).

[46] Institute for Information Infrastructure Protection, "National Cyber Security Research and Development Challenges," p. 5 (2009); *see also* CSIS Commission Report, p. 9 (recommending "overall coordination of cybersecurity research and development").

[47] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 32 (Mar. 19, 2009) (statement of Dr. Eugene Spafford).

much towards the stick rather than the carrot, thus discouraging prompt disclosures in the future. To encourage disclosure, the Defense Department should consider a combination of incentives, safe harbors, and liability limitations as mechanisms to encourage – rather than discourage – disclosing problems, sharing information, and serving as real partners to defend our information assets.

Second, the effectiveness of information sharing would be multiplied exponentially if the private sector could share not only with the Defense Department, but also with other industry partners. However, the specter of antitrust investigations and lawsuits hangs over such intra-industry cooperation. To encourage information sharing within industry, the Defense Department should consider working with industry and other agencies to define standards and safe harbors that would encourage industry cooperation leading to innovative ideas and technologies to enhance cybersecurity.

2. Fostering Technology Innovation

For homeland security, Congress recognized that protections against liability lawsuits could spur the development of anti-terrorism technologies:

> The Select Committee [on Homeland Security] believes that technological innovation is the Nation's front-line defense against the terrorist threat. Unfortunately, the Nation's products liability system threatens to keep important new technologies from the market where they could protect our citizens. In order to ensure that these important technologies are available, the Select Committee believes that it is important to adopt a narrow set of liability protections for manufacturers of these important technologies.[48]

Consistent with this legislative purpose, Congress enacted the SAFETY Act to spur the development of anti-terrorism technologies. *See* 6 U.S.C. §§ 441-44. However, this Act only covers acts of terrorism, leaving questions about its protection for other cyber attacks, such as those sponsored by nation-states and organized crime. To accelerate the fielding of new cyber technology, Congress should consider extending liability protections to the private sector producing such innovations necessary to defend against increasingly dangerous and sophisticated cyber attacks.

E. Dispute Resolution

As information systems become ever more interconnected, the Defense Department will inevitably find the need to cut off a contractor's access to the DoD network due to security breaches or inadequate security safeguards. Such actions are entirely consistent with the overall objective of protecting the security of military information assets.

---

[48] H.R. REP. NO. 107-609, Pt. 1, p. 118 (July 24, 2002).

At the same time, a contractor should not be disconnected from the DoD network if the fault lies elsewhere. In today's interconnected information world, pulling the plug on a defense network connection may effectively put a contractor out of business – *i.e.*, an information death sentence equivalent to default termination or blacklisting. Due to the serious nature of such actions, the courts and administrative forums have traditionally treated them as forfeitures that have been consistently disfavored in the law. *See, e.g.*, *Bell Helicopter Textron*, ASBCA No. 21192, 85-3 BCA ¶ 18,415 at 92,429 ("Every reasonable presumption is against a forfeiture"); *Bozied v. Brookings*, 638 N.W. 2d 264 (S.D. Sup. Ct. 2001) ("Forfeitures are considered odious in the law"); *McQueen v. Brown*, 775 A.2d 748 (N.J. Super. Ct. 2001) ("equity abhors a forfeiture").

One remedy would be to establish an administrative board with deep expertise in information security matters that could provide a prompt hearing and resolution for contractors severed from the government network. Long ago, the Defense Department opened such a forum for defense contract disputes that contractors could bring before the Armed Services Board of Contract Appeals (ASBCA). Such due process would be equally appropriate to protect contractors in the event of an unfair or improper termination from the military information network.

Conclusion

Thank you for your leadership on the Defense Department's information technology and cybersecurity initiatives that directly affect one of the most visible and vital components of America's critical infrastructure.

This concludes my statement and I would be happy to answer any questions you might have.

DCIWDMS: 10361727_1